格上基于身份的可链接环签名方案 *

刘梦情[a, b]，汪学明[b†]
(贵州大学 a. 公共大数据国家重点实验室; b. 计算机科学与技术学院, 贵阳 550025)

摘　要：为了抵抗量子算法的攻击和应对恶意签名者利用环签名技术的完全匿名性输出多个签名从而进行双重开销攻击这一缺陷，同时为了解决不必要的系统开销浪费问题，提出了一种新的格上基于身份的可链接环签名方案。该方案以格上近似最短向量问题为安全基础，将该问题的求解规约于碰撞问题的求解，利用矩阵向量间的线性运算生成签名，同时结合了基于身份的密码技术。解决了系统开销浪费问题，不涉及陷门生成和高斯采样等复杂算法，提高了签名效率，降低了存储开销，并在随机预言模型下验证了方案满足完全匿名性和强存在不可伪造性。经分析，该方案是一个安全高效的环签名方案。

关键词：可链接环签名；格；基于身份的密码体制；随机预言模型
中图分类号：TP309　　doi: 10.19734/j.issn.1001-3695.2022.03.0103

Identity-based linkable ring signature scheme from lattice

Liu Mengqing[a, b], Wang Xueming[b†]
(*a. State Key Laboratory of Public Big Data*, *b. College of Computer Science & Technology*, *Guizhou University*, *Guiyang* 550025, *China*)

Abstract: In order to resist the attack of quantum algorithm and deal with the defect that malicious signers can output multiple signatures using the complete anonymity of ring signature technology to carry out double overhead attack, and to solve the unnecessary waste of system overhead, this paper proposed a new identity-based linkable ring signature scheme form lattice. The scheme takes the approximate shortest vector problem on the lattice as the security basis, reduces the solution of the problem to the solution of the collision problem, generates the signature by using the linear operation between matrix vectors, and combines the identity-based cryptography technology. It solved the problem of system overhead waste, does not involve complex algorithms such as trapdoor generation and Gaussian sampling, improves the signature efficiency and reduces the storage overhead. It is verified that the scheme meets the requirements of complete anonymity and strong unforgeability under the random oracle model. After analysis, the scheme is a secure and efficient ring signature scheme.

Key words: linkable ring signature; lattice; identity-based cryptography; random oracle model

0　引言

电子交易方式已经成为不可阻挡的趋势，其中少不了数字签名[1]的踪影，不过签名者的身份隐私在普通的数字签名不能得到保证。针对这一问题，环签名[2]被提出并得到发展。然而，在区块链机制中，由于环签名的强匿名性，恶意签名者在相同事件上可输出两个及以上的不同签名，从而遭受双重开销攻击[3]。于是，Liu 等人[4]在 2004 年提出了具有可链接性的可链接环签名(LRS)。可链接性可以检测两个签名是否由同一用户签名。目前，LRS 已经有了很多应用，如文献[5~9]中的电子商务活动。基于身份的密码体制可以减小系统开销的浪费，首个基于身份的可链接环签名(IBLRS)[10]在 2006 年被提出。早期提出的方案[11]随后被证明有安全缺陷。目前多数传统环签名方案在量子算法出现后都有被攻破的风险，研究后量子密码学已经成为密码学的学术前沿方向。在各类后量子密码技术中，基于格的密码学以其自身的优势脱颖而出，已成为最受关注的后量子密码学技术。

基于格的密码学是由 Ajtai[12]提出的，格上的困难假设的求解对于量子计算机也是困难的[13]。2008 年，Gentry 等人[14]基于格上的难题提出了一种“hash-and-sign”签名方案，这一签名机制被广泛应用[15~18]。但是，“hash-and-sign”签名机制的存储开销和计算效率都不是很理想。除了使用“hash-and-sign”机制构造格上的环签名外，Lyubashevsky[19]给出了一个利用 Fiat-Shamir 变换基于近似最短向量问题的签名方案，此外，还提出了拒绝采样[20]技术。2018 年，Torres 等人[6]第一个后量子一次性可链接环签名。该方案基于格上困难假设 Ring-SIS，采用拒绝采样技术，提高了签名私钥的独立性，并应用在区块链交易中。同年，Baum 等人[21]提出了一种更简单、更高效的格上 LRS 方案。2019 年，Torres 等人[5]扩展了文献[6]的方案，2.0 版本的 LRS 方案诞生，并使用基于格的零知识证明实现了对超范围攻击的安全性。在 2021 年，汤永利等人[22]提出了一种采用陷门生成算法和原像采样算法的 IBLRS 方案，该方案使用的算法计算复杂，会导致时间开销增加，同时陷门尺寸较大，也会增大存储开销。

本文将构造新的格上基于身份的可链接环签名(IBLRS)方案。方案将格上近似最短向量问题的求解规约为碰撞问题的求解，不使用高斯采样或陷门技术，所有计算都是建立在矩阵向量间的简单乘法运算使其具有更高的计算效率。在随机预言机模型下验证该方案的安全性并对方案的效率进行仿真分析。

1　预备知识

1.1　符号说明

表 1 为本文中即将用到的符号的简单说明。

收稿日期：2022-03-08；**修回日期：**2022-05-05　　**基金项目：**国家自然科学基金资助项目(61163049)；贵州省自然科学基金资助项目(黔科合 J 字(7641)

作者简介：刘梦情(1996-)，女，江西高安人，硕士研究生，主要研究方向为密码学；汪学明(1965-)，男(通信作者)，安徽绩溪人，教授，硕导，博士，主要研究方向为数据挖掘、无线与移动通信、协议分析与模型检测、密码学与信息安全(gs_xmwang@163.com).

表 1　符号说明

Tab. 1　Notations

符号	说明
$\mathbb{R}(\mathbb{Z})$	实数集(整数集)
$[d]$	集合 $\{1,2,\dots,d\}$
p	素数
n	2 的次幂
m,d	整数
$\mathbb{Z}_p$	商环 $\mathbb{Z}/p\mathbb{Z}$
x^n+1	不可约多项式
$\tilde{a},\tilde{Y}\dots$	多项式
$\hat{\boldsymbol{a}},\hat{\boldsymbol{b}}\dots$	多项式向量
$\boldsymbol{A},\boldsymbol{B},\boldsymbol{C}\dots$	矩阵
$x\leftarrow S$	x 是从 S 中选择的均匀随机样本
$\\|\bullet\\|_\infty$	无穷范数
$\mathcal{H}$	哈希函数族
H	哈希函数
μ	消息

1.2　格理论

定义 1　格。设 $\boldsymbol{V}\in\mathbb{R}^{n\times m}$ 是由 $\{\boldsymbol{v}_1,\dots,\boldsymbol{v}_m\}$ 构成的矩阵，其中 $\{\boldsymbol{v}_1,\dots,\boldsymbol{v}_m\}$ 是 m 个线性无关的向量。格 $\mathcal{L}$ 由 $\boldsymbol{V}$ 生成，是指系数为 $x_m\in\mathbb{Z}^m$ 的向量 $\boldsymbol{v}_1,\dots,\boldsymbol{v}_m$ 的线性集合，即：

$$\mathcal{L}(\boldsymbol{V})=\{x_1\boldsymbol{v}_1+x_2\boldsymbol{v}_2+\cdots+x_m\boldsymbol{v}_m:x_1,x_2,\cdots,x_m\in\mathbb{Z}^m\}\tag{1}$$

设 Λ 是一个 (x^n+1)-循环格[21]，如果有 $(a_1,a_2,\cdots,a_n)\in\Lambda$，则 $(a_n,a_1,a_2,\cdots,a_{n-1})$ 也在 Λ 中。

定义 2　最短向量问题 SVP。SVP 的目标是在给定的任意格 Λ 中求解欧几里德范数最小的非零向量。简单来说，就是在给定的任意格 Λ 中，对于任意的格向量 $\boldsymbol{u}\in\Lambda$，存在这样的非零向量 $\boldsymbol{v}\in\Lambda$，使 $\\|\boldsymbol{v}\\|\le\\|\boldsymbol{u}\\|$ 成立。

定义 3　近似最短向量问题。SVP_γ 给定一个 n 维任意格 Λ，近似最短向量问题的目标是找到一个非零向量 $\boldsymbol{v}\in\Lambda$ 能使 $\\|\boldsymbol{v}\\|\le\gamma\\|\boldsymbol{u}\\|$ 成立，其中 $\boldsymbol{u}\in\Lambda$，γ 是有理数。

1.3　抗碰撞哈希函数族

定义 4[23]　抗碰撞 Hash 函数族。对于 $D\subset R$ 和整数 m，$\mathcal{H}(R,D,m)=\{h_{\hat{a}}:h_{\hat{a}}(\hat{\boldsymbol{z}})=\hat{\boldsymbol{a}}\bullet\hat{\boldsymbol{z}},\hat{\boldsymbol{a}}\in R^m,\hat{\boldsymbol{z}}\in D^m\}$ 是 Hash 函数族。等式 $h_{\hat{a}}(\hat{\boldsymbol{z}})=\hat{\boldsymbol{a}}\bullet\hat{\boldsymbol{z}}=\sum\tilde{a}_i\tilde{z}_i$ 成立，其中 $\hat{\boldsymbol{a}}=(\tilde{a}_1,\cdots,\tilde{a}_m),\hat{\boldsymbol{z}}=(\tilde{z}_1,\cdots,\tilde{z}_m)$ 且全部的计算均为环 $R=\mathbb{Z}_p[x]/\langle x^n+1\rangle$ 中的运算。

此时，给定抗碰撞 Hash 函数族 $\mathcal{H}(R,D,m)$ 中的一个 Hash 函数 h，对于任意的 $\hat{\boldsymbol{y}},\hat{\boldsymbol{z}}\in R^m$ 和 $\tilde{c}\in R$，函数 h 满足以下两个性质：

$$h(\hat{\boldsymbol{y}}+\hat{\boldsymbol{z}})=h(\hat{\boldsymbol{y}})+h(\hat{\boldsymbol{z}})\tag{2}$$

$$h(\hat{\boldsymbol{y}}\tilde{c})=h(\hat{\boldsymbol{y}})\tilde{c}\tag{3}$$

成立。

定义 5　碰撞问题 Col(h,D)。对于 $D\subset R$ 和一个给定的哈希函数 $h\in\mathcal{H}(R,D,m)$，碰撞问题的目标是找到两个满足 $h(\hat{\boldsymbol{z}}_1)=h(\hat{\boldsymbol{z}}_2)$ 的不同向量 $\hat{\boldsymbol{z}}_1,\hat{\boldsymbol{z}}_2\in D^m$。

对于任意的 (x^n+1)-循环格，碰撞问题 **Col(**h,D**)** 与 SVP_γ 的是一样困难的。

对于整数 d，定义 $D=\{\tilde{g}\in R:\\|\tilde{g}\\|_\infty\le d\}$。$\mathcal{H}(R,D,m)$ 如上所述，且 $m>\frac{\log p}{\log 2d}$，$p\ge 4dmn^{1.5}\log n$，有如下定理：

定理 1[19]　给定某个随机的哈希函数 $h\in\mathcal{H}(R,D,m)$，若是存在一个算法能以不可忽略的概率破解碰撞问题 Col(h,D)，则必定存在一个算法能够破解任意 (x^n+1)-循环格 Λ 上的 $SVP_\gamma(\Lambda)$，其中 $\gamma=16dmn\log^2 n$。

1.4　统计距离

定义 6　可忽略函数。若有这样的整数 N，给定所有的常数 c 以及 $n>N$，均有 $f(n)<n^{-c}$ 成立，则函数 f 是可忽略的。通常用 negl(n)表示可忽略函数。

定义 7　统计距离。设 X 和 Y 是有限域 S 中的两个随机变量，则变量 X 和 Y 之间的统计距离可被定义为

$$\Delta(X,Y)=\frac{1}{2}\sum_{x\in S}\left|\Pr[X=x]-\Pr[Y=x]\right|\tag{4}$$

若 X 和 Y 两者间的统计距离 $\Delta(X,Y)<\text{negl}(n)$，则称 X 与 Y 之间统计不可区分。

2　基于身份的可链接环签名

2.1　一般性定义

一个基于身份的可链接环签名方案在一般情况下都是由五个多项式时间算法(Setup、Extract、RingSign、Verify 和 Link)构成：

a)系统设置 **Setup**(n)：随机化算法，由密钥生成器 KGC 执行。该算法输入安全参数 n，得到公共参数 PP、和主私钥 MSK。

b) 私钥提取 **Extract**(PP, ID, MSK)：随机化算法，由 KGC 执行。该算法输入 PP、用户身份信息 ID 和 MSK，得到用户 ID 对应的私钥 SK_{ID}。

环签名 **RingSign**(PP，μ，ID，U, SK_{ID})：随机化算法，执行者是签名用户。该算法输入 PP、待签名消息 μ、环 U、签名者 $ID\in U$ 以及对应的 SK_{ID}，得到 μ 对应的环签名 Sig。

验证算法 **Verify**($PP, U,$ μ, Sig)：确定性算法，由验证用户执行。该算法输入公共参数 PP、环 U、消息 μ 及对应的环签名 Sig，验证通过返回“1”，不通过返回“0”。

链接算法 **Link** ((μ_1,Sig_1),(μ_2,Sig_2))：由验证者执行，该算法输入两组消息-签名对(μ_1,Sig_1)和(μ_2,Sig_2)，如果它们是由同一签名者在同一事件上生成的，则输出“link”；否则输出“unlink”。

正确性：可链接环签名的正确性表现为签名正确性和链接正确性。

签名正确性是指如果输出的是合法的签名 Sig，验证算法 **Verify** 输出“0”的概率是可忽略的，也就是：

$$\Pr\left[\text{"0"}\leftarrow\text{Verify}(PP,U,\mu,Sig)\middle|\begin{array}{c}PP,MSK\leftarrow\text{Setup}(n)\\ SK_{ID}\leftarrow\text{Extract}(PP,ID,MSK)\\ Sig\leftarrow\text{RingSign}(PP,\mu,ID,U,SK_{ID})\end{array}\right]\le\text{negl}(n)$$

链接正确性是指对于元组(μ_1,Sig_1)和(μ_2,Sig_2)，如果它们是由同一签名者在同一事件上生成的，则链接算法 **Link** 输出“unlink”的概率是可忽略的，也就是：

$$\Pr\left[\text{"unlink"}\leftarrow\text{Link}((\mu_1,Sig_1),(\mu_2,Sig_2))\middle|\begin{array}{c}PP,MSK\leftarrow\text{Setup}(n)\\ SK_{ID}\leftarrow\text{Extract}(PP,ID,MSK)\\ Sig_1\leftarrow\text{RingSign}(PP,\mu_1,ID,U_1,SK_{ID})\\ Sig_2\leftarrow\text{RingSign}(PP,\mu_2,ID,U_2,SK_{ID})\end{array}\right]\le\text{negl}(n)$$

2.2　安全模型

安全的 IBLRS 方案的需满足以下性质[24]。

定义 8　匿名性。考虑以下敌手 $\mathcal{A}$ 和挑战者 $\mathcal{C}$ 之间的游戏模拟：

初始化(***Setup***)：输入 n，$\mathcal{C}$ 执行 **Setup** 算法以获取 PP、MPK 和 MSK 并将 PP 和 MPK 发送给 $\mathcal{A}$。

询问(***Query***)：$\mathcal{A}$ 可以进行以下询问：

私钥询问(***Extract query***)：$\mathcal{A}$ 向 $\mathcal{C}$ 递交一个用户身份信息 ID，$\mathcal{C}$ 运行算法 **Extract** 返回与 ID 相应的私钥 SK_{ID}。

签名询问(***Sign query***)：$\mathcal{A}$ 向 $\mathcal{C}$ 提交一个环 $U=\{ID_1,ID_2,\cdots,ID_l\}$，用户身份信息 $ID_i\subset U$，待签名消息 μ，$\mathcal{C}$ 调用 **RingSign** 算法对消息进行签名并返回对应的签名 Sig 给敌手 $\mathcal{A}$。

挑战(***Challenge***)：完成以上查询过程之后，$\mathcal{A}$ 递交消息 μ^*，环 U^* 以及两个用户身份信息 ID_0 和 ID_1，其中 $ID_0,ID_1\subset U^*$，$\mathcal{C}$ 随机选择 $b\in\{0,1\}$，执行算法 **RingSign**，用 ID_b 对应的私钥签名消息 μ 和环 U，输出一个环签名 Sig^* 给 $\mathcal{A}$。

猜测(***Guess***)：$b^*\in\{0,1\}$ 是 $\mathcal{A}$ 得到的对随机数 b 的推测，若 $b^*=b$，则 $\mathcal{A}$ 取得游戏的胜利。

敌手 $\mathcal{A}$ 在上述游戏模型中的优势定义为

$Adv_{\mathcal{A}}^{anon}(n)=|\Pr[b^*=b]-1/2|$，若是这个优势对于任意多项式时间的 $\mathcal{A}$ 来说都是可忽略的，那么这个基于身份的可链接环签名方案满足匿名性。

定义 9　强存在性不可伪造性。考虑以下敌手 $\mathcal{A}$ 和挑战者 $\mathcal{C}$ 之间的游戏模拟：

初始化(***Setup***)：输入 n，$\mathcal{C}$ 运行 Setup 算法以获取 *PP*、*MPK* 和 *MSK* 并将 *PP* 和 *MPK* 发送给敌手 $\mathcal{A}$。

询问(***Query***)：$\mathcal{A}$ 可以进行以下询问：

哈希询问(***hash query***)：敌手 $\mathcal{A}$ 向挑战者 $\mathcal{C}$ 提交消息 μ 和环 U，$\mathcal{C}$ 返回相应的哈希值。

私钥询问(***Extract query***)：敌手 $\mathcal{A}$ 向挑战者 $\mathcal{C}$ 提交消息用户身份信息 *ID*，$\mathcal{C}$ 运行算法 **Extract** 返回 *ID* 相应的私钥 SK_{ID}。

签名询问(***Sign query***)：敌手 $\mathcal{A}$ 向挑战者 $\mathcal{C}$ 提交一个环 $U=\{ID_1,ID_2,\cdots,ID_l\}$，用户身份信息 $ID_i\subset U$ 和待签名消息 μ，$\mathcal{C}$ 调用环签名算法 **RingSign** 对消息进行签名并返回对应的签名 *Sig* 给敌手 $\mathcal{A}$。

伪造(***Forge***)：敌手 $\mathcal{A}$ 输出(μ^*,U^*,Sig^*)，如果满足以下条件：

a) $\mathcal{A}$ 之前未发起过对(μ^*,U^*)的签名查询；

b) U^* 中任一成员的私钥未被 $\mathcal{A}$ 查询过；

c)**Verify**(PP,μ^*,U^*,Sig^*) = 1。

则 $\mathcal{A}$ 成功伪造签名并赢得游戏。

$\mathcal{A}$ 在上述模拟游戏中的优势定义为 $Adv_{\mathcal{A}}^{forge}(n)=\Pr[\text{Verify}(PP,\mu^*,U^*,Sig^*)=1]$，若是这个优势对于任意 $\mathcal{A}$ 来说都是可忽略的，则称这个基于身份的可链接环签名方案满足强存在性不可伪造性。

定义 10　可链接性。考虑以下敌手 $\mathcal{A}$ 和挑战者 $\mathcal{C}$ 之间的游戏模拟：

初始化(***Setup***)：输入 n，$\mathcal{C}$ 运行 Setup 算法以获取 *PP*、*MPK* 和 *MSK* 并将 *PP* 和 *MPK* 发送给敌手 $\mathcal{A}$。

询问(***Query***)：$\mathcal{A}$ 可以进行以下询问：

哈希询问(***hash query***)：敌手 $\mathcal{A}$ 向挑战者 $\mathcal{C}$ 提交消息 μ 和环 *U*，$\mathcal{C}$ 返回相应的哈希值。

私钥询问(***Extract query***)：敌手 $\mathcal{A}$ 向挑战者 $\mathcal{C}$ 提交消息用户身份信息 *ID*，$\mathcal{C}$ 运行算法 **Extract** 返回 *ID* 相应的私钥 SK_{ID}。

签名询问(***Sign query***)：敌手 $\mathcal{A}$ 向挑战者 $\mathcal{C}$ 提交一个环 $U=\{ID_1,ID_2,\cdots,ID_l\}$，用户身份信息 $ID_i\subset U$ 和待签名消息 μ，$\mathcal{C}$ 调用环签名算法 **RingSign** 对消息进行签名并返回对应的签名 *Sig* 给敌手 $\mathcal{A}$。

伪造(***Forge***)：最后，敌手 $\mathcal{A}$ 输出元组(μ_1^*,U_1^*,Sig_1^*)和(μ_2^*,U_2^*,Sig_2^*)，如果满足以下条件：

$\mathcal{A}$ 之前未发起过对(μ_1^*,U_1^*)和(μ_2^*,U_2^*)的签名查询；

U^* 中任一成员的私钥未被 $\mathcal{A}$ 查询过；

$\mathcal{A}$ 至多拥有一个用户的私钥；

Verify(PP,μ_i^*,U_i^*,Sig_i^*)=1, $i\in\{1, 2\}$；

Link(Sig_1,Sig_2)= "unlink"。

则 $\mathcal{A}$ 赢得游戏。

$\mathcal{A}$ 在上述模拟游戏中的优势定义为 $Adv_{\mathcal{A}}^{link}(n)=\Pr[\mathcal{A}\text{ wins the game}]$，若是这个优势对于任意 $\mathcal{A}$ 来说都是可忽略的，则称这个基于身份的可链接环签名方案满足可链接性。

3　格上基于身份的可链接环签名方案

本节将构造格上 IBLRS 方案，并对方案进行分析。在构造方案之前，本文对一些变量进行说明，如表 2 所示。

3.1　方案构造

Setup(n)：给定安全参数 n，n 是 2 的次幂，$m=\log n$，$d=mn^{1.5}\log n$，$p>4d^2$ 且满足 $p=3\bmod 8$ 为素数。当 $n>4$ 时，可以验证不等式 $m>{\log p}/{\log 2d}$ 和 $p\geq 4dmn^{1.5}\log n$ 成立。从 $\mathcal{H}(R,D,m)$ 中随机选择一个 Hash 函数 h。选择一个随机预言函数 $H:\{0,1\}^*\to D_h$。从 D_s^m 随机选取 $\hat{\boldsymbol{s}}$，$\boldsymbol{C}\leftarrow R$，计算 $\tilde{S}=h(\hat{\boldsymbol{s}})$。输出 $PP=\{n,m,p,\boldsymbol{C},D,D_h,D_s,D_z,h,H\}$、$MPK=\tilde{S}$ 和 $MSK=\hat{\boldsymbol{s}}$。

Extract (*PP, ID, MSK*)：输入 *PP*、*MSK* 和用户身份信息 $ID\in\{0,1\}^*$，进行如下计算：

随机选取 $\hat{\boldsymbol{r}}_{ID}\leftarrow D^m$ 并计算 $\tilde{Q}_{ID}=h(\hat{\boldsymbol{r}}_{ID})$；

计算 $\tilde{e}=H(ID,\tilde{Q}_{ID})$ 和 $\hat{\boldsymbol{s}}_{ID}=\hat{\boldsymbol{s}}\tilde{e}+\hat{\boldsymbol{r}}_{ID}$；

如果 $\hat{\boldsymbol{s}}_{ID}\notin D_z^m$，返回步骤 1)；

输出满足 $\hat{\boldsymbol{s}}_{ID}\in D_z^m$ 和 $h(\hat{\boldsymbol{s}}_{ID})=\tilde{S}\tilde{e}+\tilde{Q}_{ID}$ (其中 $\tilde{e}=H(ID,\tilde{Q}_{ID})$)的 $\hat{\boldsymbol{s}}_{ID}$，用户身份信息 *ID* 对应的私钥是 $sk_{ID}=\hat{\boldsymbol{s}}_{ID}$。

RingSign (PP,μ,ID,sk_{ID},U)：设环 $U=\{ID_1,ID_2,\cdots,ID_l\}$。输入 *PP*，待签名消息 $\mu\in\{0,1\}^*$，签名者身份信息 $ID_j(j\in[l])$ 以及对应的签名私钥 sk_{ID_j}。签名过程如下：

计算链接标签 $I=H(\boldsymbol{C},sk_{ID_j})$；

随机选取 $\hat{\boldsymbol{y}}_j\leftarrow D_s^m$ (其中 $j\in[l]$)并计算 $\tilde{Y}=h(\hat{\boldsymbol{y}}_j)$；

计算 $\tilde{c}=H(\mu,U,\tilde{Y},ID_j)$ 和 $\hat{\boldsymbol{z}}_j=\hat{\boldsymbol{y}}_j\tilde{c}+sk_{ID_j}$；

如果 $\hat{\boldsymbol{z}}_j\notin D_z^m$，则返回步骤 1)；

输出签名 $Sig=(\hat{\boldsymbol{z}}_1,\hat{\boldsymbol{z}}_2,\cdots,\hat{\boldsymbol{z}}_l,I,\tilde{Y})$。

Verify(PP,U,μ,Sig)：给定 *PP*，$Sig=(\hat{\boldsymbol{z}}_1,\hat{\boldsymbol{z}}_2,\cdots,\hat{\boldsymbol{z}}_l,I,\tilde{Y})$，$\mu$ 和 $U=\{ID_1,ID_2,\cdots,ID_l\}$。当且仅当 $\hat{\boldsymbol{z}}_j\in D_z^m$ 且 $h(\hat{\boldsymbol{z}}_j)=\tilde{Y}\tilde{c}+\tilde{S}\tilde{e}+\tilde{Q}_{ID}$ (其中 $\tilde{c}=H(\mu,U,\tilde{Y},ID)$，$\tilde{e}=H(ID,\tilde{Q}_{ID})$)成立时，返回"1"；否则，返回"0"。

Link($\sigma_{U_1}(\mu_1)$, $\sigma_{U_2}(\mu_2)$)：输入两个环签名 $\sigma_{U_1}(\mu_1)=(\hat{\boldsymbol{z}}_1,\hat{\boldsymbol{z}}_2,\cdots,\hat{\boldsymbol{z}}_l,I_1,\tilde{Y})$ 和 $\sigma_{U_2}(\mu_2)=(\hat{\boldsymbol{z}}_1,\hat{\boldsymbol{z}}_2,\cdots,\hat{\boldsymbol{z}}_l,I_2,\tilde{Y})$。如果签名 $\sigma_{U_1}(\mu_1)$ 和 $\sigma_{U_2}(\mu_2)$ 都是有效的并且 $I_1=I_2$，则输出"link"；否则输出"unlink"。

表 2　变量说明

Tab. 2　Variables

变量	说明
R	$\mathbb{Z}_p[x]/\langle x^n+1\rangle$
D	$\{\tilde{g}\in R:\|\tilde{g}\|_\infty\leq d\}$
D_h	$\{\tilde{g}\in R:\|\tilde{g}\|_\infty\leq 1\}$
D_s	$\{\tilde{g}\in R:\|\tilde{g}\|_\infty\leq n^{0.5}\log n\}$
D_z	$\{\tilde{g}\in R:\|\tilde{g}\|_\infty\leq d-n^{0.5}\log n\}$
$\mathcal{H}(R,D,m)$	哈希函数族

3.2　正确性

下面将从签名正确性和链接正确性两个方面证明以上方案的正确性。

签名正确性：由文献[25]中的推论 6.2 可知，任意 $\hat{\boldsymbol{s}}\in D_z^m$，有 $\Pr_{\tilde{c}\leftarrow D_h}[\hat{\boldsymbol{s}}\tilde{c}+\hat{\boldsymbol{y}}\in D_z^m]=\frac{1}{e}-o(1)$ 成立，在之前的参数设定中，有 $D_z\subset D$，所以 $\hat{\boldsymbol{s}}_{ID}\in D$。由 $\hat{\boldsymbol{y}}_j\leftarrow D_s^m$ 和 $\tilde{c}\in D_h$ 可知，$\hat{\boldsymbol{z}}_j=\hat{\boldsymbol{y}}_j\tilde{c}+sk_{ID_j}$ 的概率为 $\frac{1}{e}-o(1)$。

由此可知，$\hat{\boldsymbol{z}}_j\in D_z^m$ 成立的概率是不可忽略的。签名的正确性可由以下等式验证：

$$h(\hat{\boldsymbol{z}}_j)=h(\hat{\boldsymbol{y}}_j\tilde{c}+sk_{ID})=h(\hat{\boldsymbol{y}}_j\tilde{c}+\hat{\boldsymbol{s}}\tilde{e}+\hat{\boldsymbol{r}}_{ID})=$$
$$h(\hat{\boldsymbol{y}}_j\tilde{c})+h(\hat{\boldsymbol{s}}\tilde{e})+h(\hat{\boldsymbol{r}}_{ID})=h(\hat{\boldsymbol{y}}_j)\tilde{c}+h(\hat{\boldsymbol{s}})\tilde{e}+h(\hat{\boldsymbol{r}}_{ID})=$$
$$\tilde{Y}\tilde{c}+\tilde{S}\tilde{e}+\tilde{Q}_{ID}$$

链接正确性：本文考虑两个签名 $\sigma_{U_2}(\mu_2)=(\hat{\boldsymbol{z}}_1,\hat{\boldsymbol{z}}_2,\cdots,\hat{\boldsymbol{z}}_l,I_2,\tilde{Y})$ 和 $\sigma_{U_2}(\mu_2)=(\hat{\boldsymbol{z}}_1,\hat{\boldsymbol{z}}_2,\cdots,\hat{\boldsymbol{z}}_{l'},I_2,\tilde{Y})$，其中身份信息为 $ID_i\in U_1\cap U_2$ 对两条消息 μ_1 和 μ_2 签名的诚实用户是真正的签名者，那么算法 Link 在验证的过程中一定会输出"link"。也就是说，$\Pr[I_1=I_2]=\Pr[H(\boldsymbol{C},sk_{ID_1})=H(\boldsymbol{C},sk_{ID_2})]$，其中 $sk_{ID_1}=sk_{ID_2}$，意味着 $\Pr[I_1=I_2]=1$。

综上所述，该方案满足正确性。

3.3　安全性

下面将证明该格上 IBLRS 方案的安全性。

引理 1　在随机预言模型下，该基于格的环签名方案满足完全匿名性。

证明　根据匿名性的定义，如果存在多项式时间敌手 $\mathcal{A}$ 能以不可忽略的优势 ε 赢得定义 8 中的匿名性游戏，则可构造出挑战者 $\mathcal{C}$ 调用 $\mathcal{A}$ 作为子程序以不可忽略的概率解决

SVP_γ 。$\mathcal{A}$ 与 $\mathcal{C}$ 之间的交互如下：

Setup：挑战者 $\mathcal{C}$ 进行如下操作：

确定一个最大环用户集 $U'=\{U_1,U_2,\cdots,U_{max}\}$ ，其中 *max* 表示最大用户数。

挑战者 $\mathcal{C}$ 运行 **Setup** 算法产生公开参数 *PP*、主公钥 *MPK* 和主私钥 *MSK*，并将 *PP* 和 *MPK* 发送给敌手 $\mathcal{A}$ 。

Query：敌手 $\mathcal{A}$ 可以向挑战者 $\mathcal{C}$ 发起私钥提取询问和签名询问，假设敌手 $\mathcal{A}$ 没有重复询问，$\mathcal{C}$ 的回答如下：

Extract query：敌手 $\mathcal{A}$ 向挑战者 $\mathcal{C}$ 提交用户 $ID_i \subset U'$，挑战者 $\mathcal{C}$ 运行私钥提取算法 **Extract** 返回 ID_i 对应的私钥 sk_{ID_i} 。

Sign query：敌手 $\mathcal{A}$ 向挑战者 $\mathcal{C}$ 提交一个环 $U=\{ID_1,ID_2,\cdots,ID_l\}\subset U'$、用户 $ID_i \subset U$、待签名消息 μ 以及对应的私钥 sk_{ID_i} 。挑战者 $\mathcal{C}$ 调用环签名算法 **RingSign** 对消息进行签名并返回签名 *Sig* 给 $\mathcal{A}$ 。

Challenge：完成查询后，$\mathcal{A}$ 向 $\mathcal{C}$ 提交一个消息 μ^*、环 $U^*=\{ID_1,ID_2,\cdots,ID_l\}$ 以及两个用户 $ID_{i_0},ID_{i_1}\subset U^*$，挑战者 $\mathcal{C}$ 随机选择 $b\in\{0,1\}$，运行签名算法 **RingSign** 用 ID_{i_b} 对应的私钥对 (μ^*,U^*)进行环签名并返回签名 Sig^* 给敌手 $\mathcal{A}$ 。

Guess：敌手 $\mathcal{A}$ 输出对 *b* 的猜测 $b^*\in\{0,1\}$ 。

下面说明可以忽略敌手 $\mathcal{A}$ 赢得此游戏的优势 $Adv_{\mathcal{A}}^{anon}(n)=|\Pr[b^*=b]-1/2|=\varepsilon$ 。只需要证明挑战者 $\mathcal{C}$ 用 ID_{i_b} 的私钥 SK_{i_b} 计算的环签名 $Sig^*=(\hat{\mathbf{z}}_1^*,\hat{\mathbf{z}}_2^*,\cdots,\hat{\mathbf{z}}_l^*,I^*,\tilde{Y}^*)$ 与用 $ID_{i_{1-b}}$ 的私钥 $\mathrm{SK}_{i_{1-b}}$ 计算的环签名 $Sig'=(\hat{\mathbf{z}}_1',\hat{\mathbf{z}}_2',\cdots,\hat{\mathbf{z}}_l',I',\tilde{Y}')$ 是统计不可区分的即可。

定理 2[25] 如果从 D_s^m 均匀随机选取一个 $\hat{\mathbf{s}}$，则存在另一个 $\hat{\mathbf{s}}'\in D_s^m$，有概率 $1-2^{-\Omega(n\log n)}$ 满足等式 $h(\hat{\mathbf{s}})=h(\hat{\mathbf{s}}')$ 。对于任意 $h\in\mathcal{H}(R,D,m)$、消息 μ 和任意 $\hat{\mathbf{s}},\hat{\mathbf{s}}'\in D_s^m$ 使得 $h(\hat{\mathbf{s}})=h(\hat{\mathbf{s}}')$，本文有

$$\Delta((\hat{\mathbf{z}},\tilde{c}),(\hat{\mathbf{z}}',\tilde{c}'))=n^{-\omega(1)} \quad (5)$$

由定义 7 和定理 2 可知 Sig^* 且 Sig' 是不可区分的，所以该方案满足完全匿名性。

引理 2 如果存在一个多项式时间敌手 $\mathcal{A}$ 能够以不可忽略的概率 ε 输出一个本方案的有效伪造签名，那么利用 $\mathcal{A}$ 的能力，可以构造出一个挑战者 $\mathcal{C}$，能够以至少 $(1-e^{-1}/2t)\varepsilon$ 的概率获得 **Col(*h*,*D*)**问题的一个解。其中，*e* 是自然对数，*t* 是允许敌手进行 Hash 询问的最大次数。

证明 根据强存在性不可伪造性的定义，假设存在多项式时间敌手 $\mathcal{A}$ 能以不可忽略的优势 ε 输出本方案的一个有效伪造签名，那么本文可以构造出挑战者 $\mathcal{C}$ 能够以不可忽略的概率求解 **Col(*h*,*D*)**问题。$\mathcal{A}$ 与 $\mathcal{C}$ 之间的交互如下：

Setup：挑战者 $\mathcal{C}$ 进行如下操作：

确定一个最大环用户集 $U'=\{U_1,U_2,\cdots,U_{max}\}$ ，其中 *max* 表示最大用户数。

挑战者 $\mathcal{C}$ 运行 **Setup** 算法产生公开参数 *PP*、主公钥 *MPK* 和主私钥 *MSK*，并将 *PP* 和 *MPK* 发送给敌手 $\mathcal{A}$ 。

Query：敌手 $\mathcal{A}$ 可以向挑战者 $\mathcal{C}$ 发起一系列的哈希询问和签名询问，假设敌手 $\mathcal{A}$ 没有重复询问，$\mathcal{C}$ 的回答如下：

Hash query：挑战者 $\mathcal{C}$ 维护两个初始均为空的列表 L_1 和 L_2，列表 L_1 的元组为 $(ID_i,\tilde{Q}_{ID_i},\tilde{e}_i)$，列表 L_2 的元组为 $(\mu_i,ID_i,U,\tilde{Y}_i,\tilde{c}_i)$ 。敌手 $\mathcal{A}$ 随机选取 *l* 个向量 $\hat{\mathbf{y}}_i\leftarrow D_s^m$，$i\in[l]$，随后向挑战者 $\mathcal{C}$ 提交一个消息 μ_i、环 $U=\{ID_1,ID_2,\cdots,ID_l\}$ 和身份信息 ID_i 进行询问。当敌手 $\mathcal{A}$ 对 $(ID_i,\tilde{Q}_{ID_i})$ 进行哈希询问时，$\mathcal{C}$ 检查列表 L_1，假如 $(ID_i,\tilde{Q}_{ID_i},\tilde{e}_i)$ 存在，则直接将 $\tilde{e}_i$ 返回给 $\mathcal{A}$；否则，$\mathcal{C}$ 随机返回 $\tilde{e}_i$ 给 $\mathcal{A}$，并在列表 L_1 中添加 $(ID_i,\tilde{Q}_{ID_i},\tilde{e}_i)$ 。当敌手 $\mathcal{A}$ 对 $(\mu_i,ID_i,\tilde{Y}_i)$ 进行哈希询问时，$\mathcal{C}$ 检查列表 L_2，假如 $(\mu_i,ID_i,U,\tilde{Y}_i,\tilde{c}_i)$ 存在，则直接将 $\tilde{c}_i$ 返回给 $\mathcal{A}$；否则，$\mathcal{C}$ 随机返回 $\tilde{c}_i$ 给 $\mathcal{A}$，并在列表 L_2 中添加 $(\mu_i,ID_i,U,\tilde{Y}_i,\tilde{c}_i)$ 。

Extract query：挑战者 $\mathcal{C}$ 维护初始为空的列表 L_3，列表 L_3 的元组为 $(ID_i,sk_{ID_i},\tilde{Q}_{ID_i},\tilde{e}_i)$ 。当敌手 $\mathcal{A}$ 对 $(ID_i,\tilde{Q}_{ID_i},\tilde{e}_i)$ 进行私钥提取询问时，$\mathcal{C}$ 检查列表 L_3，假如 $(ID_i,sk_{ID_i},\tilde{Q}_{ID_i},\tilde{e}_i)$ 存在，则直接将 $(sk_{ID_i},\tilde{Q}_{ID_i})$ 返回给 $\mathcal{A}$；否则，$\mathcal{C}$ 随机选择 $sk_{ID_i}\in D_z^m$ 并计算 $\tilde{Q}_{ID_i}=h(sk_{ID_i})-\tilde{S}\tilde{e}_i$，其中 $\tilde{e}_i$ 从哈希询问中获得，返回 $(sk_{ID_i},\tilde{Q}_{ID_i})$ 给 $\mathcal{A}$，并在列表 L_1 和列表 L_3 中分别添加 $(ID_i,\tilde{Q}_{ID_i},\tilde{e}_i)$ 和 $(ID_i,sk_{ID_i},\tilde{Q}_{ID_i},\tilde{e}_i)$ 。

Sign query：挑战者 $\mathcal{C}$ 维护初始为空的列表 L_4，列表 L_4 的元组为 $(\mu_i,ID_i,U,\tilde{Y}_i,\tilde{c}_i,I,\hat{\mathbf{z}}_i)$ 。敌手 $\mathcal{A}$ 随机选取 *l* 个向量 $\hat{\mathbf{y}}_i\leftarrow D_s^m$，$i\in[l]$，随后向挑战者 $\mathcal{C}$ 提交一个消息 μ_i、环 $U=\{ID_1,ID_2,\cdots,ID_l\}$ 和身份信息 $ID_i\subset U$ 进行询问。当敌手 $\mathcal{A}$ 对 (μ_i,ID_i,U) 进行签名询问时，$\mathcal{C}$ 检查列表 L_4，假如 $(\mu_i,ID_i,U,\tilde{Y}_i,\tilde{c}_i,I,\hat{\mathbf{z}}_i)$ 存在，则直接将 $(\tilde{Y}_i,\hat{\mathbf{z}}_i)$ 返回给 $\mathcal{A}$；否则，$\mathcal{C}$ 检查列表 L_3，如果 $(ID_i,sk_{ID_i},\tilde{Q}_{ID_i},\tilde{e}_i)$ 不存在，则对 $(ID_i,\tilde{Q}_{ID_i},\tilde{e}_i)$ 进行私钥提取询问以获得与 ID_i 对应的 $(sk_{ID_i},\tilde{Q}_{ID_i})$ 。接下来，$\mathcal{C}$ 随机选择 $\hat{\mathbf{y}}_i\leftarrow D_s^m$ ($i\in[l]$)，并计算 $\tilde{Y}_i=h(\hat{\mathbf{y}}_i)$ 和 $\hat{\mathbf{z}}_i=\hat{\mathbf{y}}_i\tilde{c}_i+sk_{ID_i}$，其中 $\tilde{c}_i$ 从哈希询问中获得。最后，$\mathcal{C}$ 返回 $(\mu_i,ID_i,U,\hat{\mathbf{z}}_i)$ 给 $\mathcal{A}$，并在列表 L_2 和列表 L_4 中分别添加 $(\mu_i,ID_i,U,\tilde{Y}_i,\tilde{c}_i)$ 和 $(\mu_i,ID_i,U,\tilde{Y}_i,\tilde{c}_i,I,\hat{\mathbf{z}}_i)$ 。

Forge：敌手 $\mathcal{A}$ 完成上述询问后以不可忽略的概率 ε 输出 $(\mu^*,U^*,\hat{\mathbf{z}}^*,\tilde{e}^*)$ 这样一个有效伪造签名。其中，敌手 $\mathcal{A}$ 从未发起过对 $(\mu^*,U^*,ID^*,sk_{ID}^*)$ 的签名查询，也未查询过 U^* 中任一用户的私钥。

文献[26,27]中的分叉引理表明，$\mathcal{A}$ 能输出两个有效伪造签名 $(\mu^*,U^*,\hat{\mathbf{z}}_1^*,\tilde{e}_1^*)$ 和 $(\mu^*,U^*,\hat{\mathbf{z}}_2^*,\tilde{e}_2^*)$ 的概率 $\varepsilon^*\geq\frac{1-e^{-1}}{2t}\varepsilon$ 不可忽略，且满足 $\tilde{e}_1^*\neq\tilde{e}_2^*$ 。

在这样的情况下，$h(\hat{\mathbf{z}}_1^*)=\tilde{Y}^*\tilde{c}^*+\tilde{S}\tilde{e}_1^*+\tilde{Q}_{ID^*}$ 且 $h(\hat{\mathbf{z}}_2^*)=\tilde{Y}^*\tilde{c}^*+\tilde{S}\tilde{e}_2^*+\tilde{Q}_{ID^*}$ 。从而 $h(\hat{\mathbf{z}}_1^*-MSK\tilde{e}_1^*)=h(\hat{\mathbf{z}}_2^*-MSK\tilde{e}_2^*)$ 成立的概率不小于 1/2。由此，能够以 $\varepsilon^*\cdot\frac{1}{2}\geq\frac{1-e^{-1}}{2t}\varepsilon$ 的概率得到关于 *h* 的碰撞。

因此，若敌手 $\mathcal{A}$ 成功得到一个本方案的有效伪造签名，那么挑战者 $\mathcal{C}$ 就能求解出 **Col(*h*,*D*)**问题。根据 1.3 节中的定理 1 和 3.3 节中的引理 2，本方案满足强存在不可伪造性。

引理 3 若方案不可伪造，则该方案满足可链接性。

证明 根据可链接性的定义，假设存在多项式时间敌手 $\mathcal{A}$ 能以不可忽略的优势 ε 赢得定义 10 中的可链接性模拟游戏。$\mathcal{A}$ 与 $\mathcal{C}$ 之间的交互如下：

Setup：挑战者 $\mathcal{C}$ 执行如下操作：

确定一个最大环用户集 $U'=\{U_1,U_2,\cdots,U_{max}\}$ ，其中 *max* 表示最大用户数。

挑战者 $\mathcal{C}$ 运行 **Setup** 算法产生公开参数 *PP*、主公钥 *MPK* 和主私钥 *MSK*，并将 *PP* 和 *MPK* 发送给敌手 $\mathcal{A}$ 。

Query：敌手 $\mathcal{A}$ 可以向挑战者 $\mathcal{C}$ 发起一系列询问，假设敌手 $\mathcal{A}$ 没有重复询问，$\mathcal{C}$ 的回答如下：

Hash query：敌手 $\mathcal{A}$ 对 ID_i 发起哈希询问时，$\mathcal{C}$ 返回 $\tilde{e}_i$ 和 $\tilde{c}_i$ 给 $\mathcal{A}$ 。

Extract query：敌手 $\mathcal{A}$ 对 ID_i 进行私钥提取询问，$\mathcal{C}$ 返回 sk_{ID_i} 给 $\mathcal{A}$ 。

Sign query：敌手 $\mathcal{A}$ 向挑战者 $\mathcal{C}$ 提交一个消息 μ_i、环 $U=\{ID_1,ID_2,\cdots,ID_l\}$ 和身份信息 $ID_i\subset U$ 进行询问，$\mathcal{C}$ 返回 $(\tilde{Y},I_i,\hat{\mathbf{z}}_i)$ 给 $\mathcal{A}$ 。

Forge：敌手 $\mathcal{A}$ 完成上述询问后输出 $\sigma_{U_1}(\mu_1)=(\hat{\mathbf{z}}_1,\hat{\mathbf{z}}_2,\cdots,\hat{\mathbf{z}}_l,I_1,\tilde{Y})$ 和 $\sigma_{U_2}(\mu_2)=(\hat{\mathbf{z}}_1,\hat{\mathbf{z}}_2,\cdots,\hat{\mathbf{z}}_l,I_2,\tilde{Y})$ 。

分析：假设敌手 $\mathcal{A}$ 在只拥有一个私钥的情况下能够以不可忽略的概率 ε 生成两个环签名 $\sigma_{U_1}(\mu_1)$ 和 $\sigma_{U_2}(\mu_2)$，并且 **Verify** $(PP,\mu_i,\sigma_{U_i}(\mu_i),U_i)$ 总是输出“1”。由于本方案不可伪造，所以，当敌手 $\mathcal{A}$ 按照规则诚实地输出签名 $\sigma_{U_1}(\mu_1)$ 和 $\sigma_{U_2}(\mu_2)$ 时，这两个签名才能通过验证算法并输出“1”。换句话说，有 $I_1=H(\mathbf{C},sk_{ID_1})$ 和 $I_2=H(\mathbf{C},sk_{ID_2})$，$\mathcal{A}$ 只拥有一个私钥，即 $sk_{ID_1}=sk_{ID_2}$，则随机预言机 *H* 有相同的输出，即 $I_1=I_2$ 。表明签名 $\sigma_{U_1}(\mu_1)$ 和 $\sigma_{U_2}(\mu_2)$ 经链接算法 **Link** 验证时会输出“link”，这与定义 10

中的假设矛盾，$\mathcal{A}$ 赢得游戏的优势 $Adv_{\mathcal{A}}^{link}(n)$ 是可忽略的，所以方案是可链接的。

3.4　效率分析

本节将主要从时间开销和存储开销两方面比较本方案与现有的几个方案的效率并分析，比较对象为文献[6,21,22]中的方案。

四种方案的时间开销比较结果如表 3 所示，其中 l 表示环成员数，T_{TG}，T_{SP}，T_{SD}，T_{BD}，T_{LHL} 和 T_{MV} 分别表示算法 TrapGen, SamplePre, SampleDom, BasisDel, 剩余哈希定理(LHL)和矩阵向量之间操作的平均时间消耗，主要对主密钥输出(MK)、用户密钥输出(UK)、签名输出(Sig)和验证(Ver)等过程的耗时进行分析。在 MK 方面，本方案和文献[22]中方案涉及基于身份的密码体制，文献[22]使用陷门生成算法生成主密钥，时间开销是 T_{TG}。本文的方案不涉及陷门生成算法，时间开销为 T_{MV}。文献[6,21]的方案不是基于身份的方案，因此不存在该部分时间开销。在 UK 方面，本文的方案使用一个耗时较短的 hash 函数来输出公钥，然后进行简单的矩阵向量之间运算来输出私钥。因此，可以忽略公钥的输出时间，而私钥的生成时间为 T_{MV}。对于文献[6,21]方案，用户公钥是通过随机选择的矩阵和向量的标量乘法生成的。文献[6]中的方案的私钥是使用 LHL 产成的，文献[21]中的方案利用 SampleDom 算法生成私钥。文献[22]中的方案使用一个耗时较短的哈希函数来生成用户的公钥，并调用 SamplePre 算法来生成用户的私钥。因此，用户密钥生成需要 T_{SP}。在 Sig 方面，本文的方案生成的签名是 $Sig=(\hat{z}_1,\hat{z}_2,\cdots,\hat{z}_l,I,\hat{Y})$，执行矩阵和向量的乘法操作即可。经过比较，本文的方案的签名生成时间开销远小于其他三种方案。在 Ver 方面，只需要矩阵和向量的乘法操作。经过比较，该方案的签名验证效率比其他三种参考方案更高。

四种方案的存储开销比较结果如表 4 所示，其中 l 表示环成员数。主要分析公钥、私钥和签名的大小。在公钥方面，本文的方案对用户的身份信息执行哈希操作输出一个 n 维列向量作为用户的公钥。文献[6]方案进行 $n\times(m-1)$ 维矩阵和 $(m-1)$ 维列向量的乘法运算生成 n 维列向量作为用户公钥。文献[21]方案进行 $n\times m$ 维矩阵和m维列向量的乘法运算生成 n 维列向量作为用户公钥。文献[22]的方案对用户的身份信息执行哈希操作输出一个 n 维的列向量作为用户公钥。在私钥方面，本方案的用户私钥是通过矩阵向量之间的标量乘法计算的，是一个m维列向量。文献[6]方案通过调用 **BasisDel** 算法和 **SamplePre** 算法，生成为 $m\times k$ 维矩阵作为私钥。文献[21]的方案通过调用 **LHL**，输出 $(m-1)$ 维列向量作为私钥。文献[22]的方案通过调用 **SamplePre** 算法生成m维列向量作为私钥。在签名大小方面，本方案生成的签名中的向量 $\hat{z}_i\,(i=1,2,\cdots,l)$ 和 $\hat{Y}$ 都是 m 维的列向量。分析结果表明，本方案在签名大小上优于其他方案。

表 3　时间开销比较

Tab. 3　Comparison of time costs

方案	MK	UK	Sig	Ver
方案[6]	/	$T_{LHL}+T_{MV}$	$(3l+2)T_{MV}+lT_{SD}$	$(4l+1)T_{MV}$
方案[21]	/	$T_{SD}+T_{MV}$	$(2l+1)T_{MV}+lT_{SD}$	$3lT_{MV}$
方案[22]	T_{TG}	T_{SP}	$(2l+1)T_{MV}+lT_{SD}$	$2lT_{MV}$
本文方案	T_{MV}	T_{MV}	lT_{MV}	lT_{MV}

表 4　存储开销比较

Tab. 4　Comparison of storage overhead

方案	公钥	私钥	签名
方案[6]	$n\log q$	$(m-1)\log q$	$(ml+n)\log q$
方案[21]	$n\log q$	$m\log q$	$(ml+n)\log q$
方案[22]	$n\log q$	$m\log q$	$[(m+1)l+n]\log q$
本文方案	$m\log p$	$m\log p$	$m(l+1)\log p$

设置参数 $n=8$，$m=640$，$q=2^{32}=4294967296$，$k=6$，硬件环境为 Windows 10 操作系统、AMD Ryzen 5 4600U with Radeon Graphics 2.10 GHz 处理器，编译环境为 Python3.9、JetBrains PyCharm 2018.1.3 x64，在此条件下进行仿真实验。表 5 和表 6 为参考方案及本方案在环成员数分别为 8、32、128 的情况下的时间开销和存储开销对比结果，由于公钥和私钥尺寸不受环成员数影响，此处存储开销为签名尺寸的对比。图 1 为实验结果对比图，其中(a)(b)(c)分别表示环成员数为 8、32、128 的结果图。综合分析，本方案较其他三个参考方案在时间开销和存储开销上均有所提升。

表 5　时间开销比较(ms)

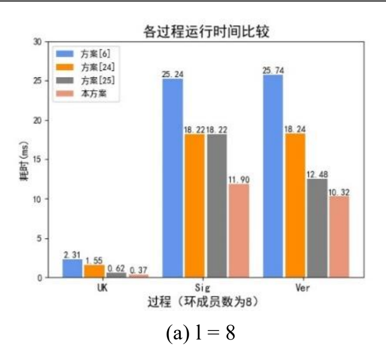
Tab. 5　Comparison of time costs(ms)

方案	$l=8$			$l=32$			$l=8$		
	UK	Sig	Ver	UK	Sig	Ver	UK	Sig	Ver
方案[6]	2.31	25.24	25.74	2.31	78.53	79.44	2.31	315.74	317.24
方案[21]	1.55	18.22	18.24	1.55	60.26	57.68	1.55	238.82	235.43
方案[22]	0.62	18.22	12.48	0.62	60.26	38.72	0.62	238.82	155.62
本文方案	0.37	11.90	10.32	0.37	45.17	28.93	0.37	185.26	126.91

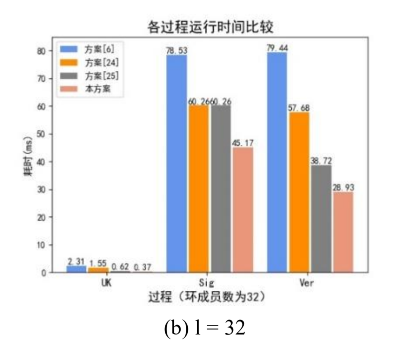
表 6　签名尺寸比较(KB)

Tab. 6　Comparison of signature sizes(KB)

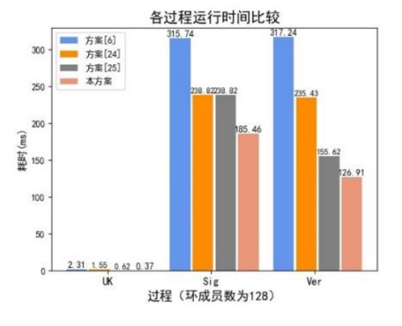
方案	l = 1	l = 8	l = 32	l = 128
方案[6]	7.46	59.83	235.62	942.18
方案[21]	7.46	59.83	235.62	942.18
方案[22]	7.47	60.91	235.93	943.46
本文方案	6.74	55.01	213.07	852.03



(a) l = 8



(b) l = 32



(c) l =128

图 1　时间开销比较(ms)

Fig. 1　Comparison of time costs(ms)

4 结束语

基于格的环签名的研究具有巨大的潜力和广阔的前景。然而，现有的大多数基于格的环签名方案都存在计算效率低、存储开销大等缺陷。与此同时，基于身份的可链接环签名实现了基于身份的密码体制和环签名技术的结合，有效地减小了系统开销浪费问题。同时，为了应对抵抗量子算法攻击的潜在风险，本文的方案结合了格密码学中的 SVP 难题，对其求解难度等价于循环格上碰撞问题的的求解，在方案的构造过程中没有使用抽样算法和陷门算法，均为矩阵向量之间的简单乘法运算，这极大程度地降低了计算复杂度，减少了各步骤的运行时间和降低了存储开销。在随机预言模型下，给出了严格的安全证明，方案满足匿名性、不可伪造性和可链接性。与现有的方案相比，该方案的效率在各方面都得到了提升。

参考文献：

[1] Diffie W, Hellman M. New directions in cryptography [J]. IEEE Transactions on Information Theory, 1976, 22 (6): 644-654.

[2] Rivest R L, Shamir A, Tauman Y. How to leak a secret [C]// Advances in Cryptology — ASIACRYPT 2001. Cambridge MA: Laboratory for Computer Science, Massachusetts Institute of Technology, 2001: 552-565.

[3] B Forum. GHash. IO and Double-Spending Against BetCoin Dice [EB/OL]. (2020-07-23) [2022-04-26]. https://bitcointalk. org/index. php?topic=327767. 0.

[4] Liu J K, Wei V K, Wong D S. Linkable Spontaneous Anonymous Group Signature for Ad Hoc Groups [C]// Australasian Conference on Information Security and Privacy. Berlin: Springer-Verlag, 2004: 325-335.

[5] Torres W A, Kuchta V, Steinfeld R, *et al.* Lattice RingCT V2. 0 with Multiple Input and Multiple Output Wallets [J]. Springer, Cham, 2019, 11547: 156–175.

[6] Alberto Torres W A, Steinfeld R, Sakzad A, *et al.* Post-quantum one-time linkable ring signature and application to ring confidential transactions in blockchain (Lattice RingCT v1. 0) [J]. Springer, Cham, 2018, 10946: 558-576.

[7] Shen N, Mackenzie A, Lab T M. Ring confidential transactions [J]. Ledger, 2016, 1: 1–18.

[8] Sun S F, Au M H, Liu J K, *et al.* RingCT 2. 0: A compact accumulator-based (linkable ring signature) protocol for blockchain cryptocurrency monero [C]// Computer Security – ESORICS 2017, LNCS. Springer, Cham. 2017, 10493: 456–474.

[9] Yuen T H, Sun S F, Liu J K, *et al.* RingCT 3. 0 for blockchain confidential transaction: Shorter size and stronger security [C]// Financial Cryptography and Data Security. FC 2020, LNCS. Springer, Cham. 2020, 12059: 464-483.

[10] Chow S, Susilo W, Yuen T H. Escrowed linkability of ring signatures and its applications [C]// Progress in Cryptology-VIETCRYPT 2006, LNCS. Berlin: Springer. 2006, 4341: 175–192.

[11] Jeong I R, Kwon J O, Dong H L. Analysis of Revocable-iff-Linked Ring Signature Scheme [J]. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2009, 92 (1): 322-325.

[12] Ajtai M. Generating hard instances of lattice problems (extended abstract) [C]// Proceedings of the twenty-eighth annual ACM symposium on Theory of Computing (STOC'96) , ACM, New York, NY, USA. 1996: 99–108.

[13] Regev O. Lattice-Based Cryptography [C]// Advances in Cryptology-CRYPTO 2006, LNCS. Berlin: Springer. 2006, 4117: 131-141.

[14] Gentry C, Peikert C, Vaikuntanathan V. Trapdoors for hard lattices and new cryptographic constructions [C]// Proceedings of the 40th Annual ACM Symposium on Theory of Computing, Victoria, British Columbia, Canada. 2008: 197–206.

[15] Wang Fenghe, Hu Yupu, Wang Chunxiao. A Lattice-based Ring Signature Scheme from Bonsai Trees [J]. Journal of Electronics and Information Technology. 2010, 32 (10): 2400–2403.

[16] Wang Jin, Sun Bo. Ring Signature Schemes from Lattice Basis Delegation [C]// Information and Communications Security-13th International Conference, ICICS 2011, LNCS. Berlin: Springer. 2011, 7043: 15-28.

[17] Zhang Lili, Ma Yanqin. A Lattice-Based Identity-Based Proxy Blind Signature Scheme in the Standard Model [J]. Mathematical Problems in Engineering, 2014 (1): Article ID 307637.

[18] Lai R, Cheung H, Chow S. Trapdoors for Ideal Lattices with Applications [C]// Information Security and Cryptology. Inscrypt 2014, LNCS. Springer, Cham. 2015, 8957: 239-256.

[19] Lyubashevsky V. Fiat-Shamir with Aborts: Applications to Lattice and Factoring-Based Signatures [C]// International Conference on the Theory and Application of Cryptology and Information Security. Berlin: Springer. 2009, 5912: 598-616.

[20] Lyubashevsky V. Lattice signatures without trapdoors [C]// Advances in Cryptology – EUROCRYPT 2012, LNCS. Berlin: Springer. 2012, 7237: 738–755.

[21] Baum C, Lin H, Oechsner S. Towards Practical Lattice-Based One-Time Linkable Ring Signatures [C]// Information and Communications Security. ICICS 2018. LNCS. Springer, Cham. 2018, 11149: 303-322.

[22] 汤永利，夏菲菲，叶青，等. 格上基于身份的可链接环签名 [J]. 密码学报, 2021, 8 (2): 232－247. (Tang Yongli, Xia Feifei, Ye Qing, *et al.* Identity-based linkable ring signature on lattice [J]. Journal of Cryptologic Research, 2021, 8 (2): 232－247.)

[23] Lyubashevsky V, Micciancio D. Generalized Compact Knapsacks Are Collision Resistant [C]// Automata, Languages and Programming. ICALP 2006, LNCS. Berlin: Springer. 2006, 4052: 144-155.

[24] Micciancio D. Generalized compact knapsacks, cyclic lattices, and efficient one-way functions [J]. Comput Compl, 2007, 16 (4): 365-411.

[25] Lyubashevsky V. Towards practical lattice-based cryptography [D]. University of California at San Diego University of California at San Diego, 2008.

[26] Pointcheval D, Stern J. Security Arguments for Digital Signatures and Blind Signatures [J]. Journal of Cryptology, 2000, 13 (3): 361–396.

[27] Bellare M, Neven G. Multi-signatures in the Plain public-Key Model and a General Forking Lemma [C]// Proceedings of the 13th ACM Conference on Computer and Communications Security, ACM, New York, NY, USA. 2006: 390-399.